Title	Crossed homomorphisms and the Schur-Zassenhaus theorem (Cohomology Theory of Finite Groups and Related Topics)
Author(s)	Asai, Tsunenobu; Takegahara, Yugen; Chigira, Naoki; Niwasaki, Takashi
Citation	数理解析研究所講究録 (2004), 1357: 23-30
Issue Date	2004-02
URL	http://hdl.handle.net/2433/25197
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録 1357 巻 2004 年 23-30

Crossed homomorphisms and the Schur-Zassenhaus theorem

近畿大学・理工学部　淺井 恒信 (Tsunenobu Asai)
Department of Mathematics, Kinki University
室蘭工業大学　竹ヶ原 裕元 (Yugen Takegahara)
千吉良 直紀 (Naoki Chigira)
Muroran Institute of Technology
愛媛大学・理学部　庭崎 隆 (Takashi Niwasaki)
Department of Mathematics, Ehime University

1 Theorems

We can find several proofs, for example, in [6–13], of the following classical theorem of Frobenius:

Theorem 1.1 (Frobenius). *Let n be an integer and G a finite group. Then*

$$\left|\{g \in G \mid g^n = 1\}\right| \equiv 0 \pmod{\gcd(n, |G|)},$$

where $|X|$ denotes the cardinality of a set X.

This theorem is equivalent to the fact that

$$|\mathrm{Hom}(C, G)| \equiv 0 \pmod{\gcd(|C|, |G|)}$$

for any finite cyclic group C, where Hom denotes the set of group homomorphisms. Yoshida has generalized the theorem as follows:

Theorem 1.2 (Yoshida [12]). *Let A be a finite abelian group and G a finite group. Then*

$$|\mathrm{Hom}(A, G)| \equiv 0 \pmod{\gcd(|A|, |G|)}.$$

Another way of generalization is due to P. Hall:

Theorem 1.3 (P. Hall [10]). *Let G be a finite group and θ an automorphism of G. If the order of θ divides a positive integer n, then*

$$\left|\{g \in G \mid g \cdot \theta(g) \cdot \theta^2(g) \cdots \theta^{n-1}(g) = 1\}\right| \equiv 0 \pmod{\gcd(n, |G|)}.$$

The theorem of Frobenius corresponds to the case $\theta = 1$. We reform this Hall's generalization in terms of '$Z^1(A, G)$' as well as Theorem 1.1 in terms of $\mathrm{Hom}(A, G)$, as follows.

Let a group A act on a group G by a group homomorphism $\varphi\colon A \to \mathrm{Aut}(G)$, where $\mathrm{Aut}(G)$ is the automorphism group of G. For $a \in A$ and $g \in G$, we indicate $\varphi(a)(g)$ by ${}^a g$. A map $\lambda\colon A \to G$ is called a *crossed homomorphism* or a *derivation* (with respect to φ) provided

$$\lambda(ab) = \lambda(a) \cdot {}^a\lambda(b) \quad \text{for all } a, b \in A.$$

We denote by $Z^1(A,G)$ the set of crossed homomorphisms from A to G. For example, the zero map $0\colon A \to G$ sending all the elements of A onto $1 \in G$ is a crossed homomorphism. If the action φ is trivial, then $Z^1(A,G) = \mathrm{Hom}(A,G)$. On the other hand, if G is abelian, then $Z^1(A,G)$ coincides with the first cocycle group of the $\mathbb{Z}A$-module G with respect to the standard resolution of A. However, unless G is abelian, $Z^1(A,G)$ may be only a set; it may not have a group structure in general.

Now, Hall's theorem is equivalent to the fact that

$$\left|Z^1(C,G)\right| \equiv 0 \pmod{\gcd(|C|,|G|)}$$

for any finite cyclic group C and for any action of C on G. Yoshida and the first author of this report have conjectured the following:

Conjecture 1.4 ([5]). If a finite group A acts on a finite group G, then

$$\left|Z^1(A,G)\right| \equiv 0 \pmod{\gcd(|A/A'|,|G|)},$$

where A' denotes the commutator subgroup of A.

This conjecture is a generalization of all the theorems above, and is still open. Recent progress for this conjecture is found in [1–4]. In particular, in order to prove the conjecture completely, it suffices to prove the conjecture in the case where A is an abelian p-group and G is a p-group for a prime p ([1]). This reduction mainly owes to the functorial properties of $Z^1(A,G)$ on the variables A and G, where the latter is first observed by Brauer [6] in a certain case (see §3.3 for generalization). In addition, Brauer has based his alternative proof of the theorem of Frobenius on the following lemma:

Lemma 1.5 (Brauer [6]). *Let G be a finite normal subgroup of a group E. Then, for any $g \in G$ and $x \in E$, $(gx)^{|G|}$ and $x^{|G|}$ is conjugate by an element of G.*

In this report, we shall generalize this Brauer's lemma as the formula

$$\mathrm{res}_{A,A^{|G|}}(Z^1(A,G)) = B^1(A^{|G|},G)$$

for abelian A (Theorem 4.1), where B^1 denotes the set of coboundaries, which will be introduced in the next section. Throughout the report, our main tools are the functorial properties of $Z^1(A,G)$, and our principle is to compare $Z^1(A,G)$ with $B^1(A,G)$. As a corollary of our arguments together with the Feit-Thompson theorem, we shall also prove Theorem 4.2 which is equivalent to the second statement of the following classical theorem:

Theorem 1.6 (Schur-Zassenhaus). *Let G be a finite normal subgroup of a finite group E such that* $\gcd(|E:G|,|G|)=1$. *Then*

(1) *There exists a subgroup A of E such that $E = G \rtimes A$.*
(2) *If $E = G \rtimes A = G \rtimes B$, then A and B are conjugate by an element of G.*

Note that if G is abelian, then it is well known that the first statement of the Schur-Zassenhaus theorem is equivalent to $H^2(A,G)=0$, and the second is so to $H^1(A,G)=0$. In fact, we shall prove $Z^1(A,G) = B^1(A,G)$ for any finite group A and G whose orders are relatively prime.

Notation. For the remainder of the report, we fix the following notation: let A and G be groups, which need not be finite, and let A act on G by a group homomorphism $\varphi\colon A \to \mathrm{Aut}(G)$. With respect to this action φ, we denote by $Z^1(A,G)$ the set of crossed homomorphisms from A to G, and by $G \rtimes A$ the semidirect product of G and A. For $x \in G \rtimes A$, we denote by $\mathrm{Inn}(x)$ the inner automorphism associated with x, so that $\mathrm{Inn}(x)(y) = {}^x y = xyx^{-1}$ for all $y \in G \rtimes A$.

2 Coboundaries

For a given map $\lambda\colon A \to G$, consider the map $\tilde{\lambda}\colon A \to G \rtimes A$ which is defined by

$$\tilde{\lambda}(a) = \lambda(a)a \quad \text{for all } a \in A.$$

It is easy to show that $\lambda \in Z^1(A,G)$ if and only if $\tilde{\lambda} \in \mathrm{Hom}(A, G \rtimes A)$, and in this case, $\tilde{\lambda}$ becomes a splitting monomorphism of the canonical epimorphism $\pi\colon G \rtimes A \to A$. On the other hand, any splitting monomorphism θ of π defines a complement $\theta(A) \leq G \rtimes A$ of G, and vice versa. From these observations, we obtain the following well-known result:

Theorem 2.1. *There are two bijections*

$$\begin{aligned} Z^1(A,G) &\xrightarrow{\Phi} \{\theta \in \mathrm{Hom}(A, G \rtimes A) \mid \pi \circ \theta = \mathrm{id}_A\} \\ &\xrightarrow{\Psi} \{B \leq G \rtimes A \mid GB = G \rtimes A,\ G \cap B = 1\}, \end{aligned}$$

where $\Phi(\lambda) = \tilde{\lambda}$ *and* $\Psi(\theta) = \theta(A)$.

As in homological algebra, we introduce the concept of 'coboundary' as well as cocycle. For arbitrary $g \in G$ and $a \in A$, regarding them as elements in $G \rtimes A$, we consider their commutator $[g,a]$, where

$$[g,a] = gag^{-1}a^{-1} = g \cdot {}^a(g^{-1}) \in G.$$

Then this induces a map $[g,-]\colon A \to G$ sending $a \in A$ to $[g,a] \in G$. We call this map $[g,-]$ a *coboundary* or an *inner derivation* induced from g (with respect to φ), and set

$$B^1(A,G) = \{[g,-] \mid g \in G\}.$$

Easy calculation shows that $B^1(A,G) \subseteq Z^1(A,G)$. In fact, if G is abelian, then $B^1(A,G)$ coincides with the first coboundary group of the $\mathbb{Z}A$-module G with respect to the standard resolution of A. However, in general cases, $B^1(A,G)$ may not have a group structure. Our principle of this report is to compare $B^1(A,G)$ with $Z^1(A,G)$. First we emphasize the following lemma on the relation between the coboundary $[g,-]$ and conjugation by g. Since $[g,a]a = {}^g a$ in $G \rtimes A$, we have

Lemma 2.2. *Given* $g \in G$, *set* $\gamma = [g,-]$. *Then* $\tilde{\gamma}(a) = {}^g a$ *for all* $a \in A$.

In other words, $\Phi([g,-]) = \mathrm{Inn}(g)$ on A. Note that ${}^g A \neq A$ in general.

3 Parameters

Both $Z^1(A,G)$ and $B^1(A,G)$ have three parameters: groups A, G and action φ. We shall consider functorial properties on these parameters.

3.1 Change of actions

We fix $\lambda \in Z^1(A,G)$. For given $a \in A$, the inner automorphism $\mathrm{Inn}(\tilde{\lambda}(a))$ on $G \rtimes A$ leaves the normal subgroup G invariant. This induces a new action $\mathrm{Inn}\,\tilde{\lambda}\colon A \to \mathrm{Aut}(G)$, namely,

$$(\mathrm{Inn}\,\tilde{\lambda})(a)(g) = {}^{\tilde{\lambda}(a)}g = {}^{\lambda(a)}({}^{a}g) \quad \text{for } a \in A \text{ and } g \in G.$$

We denote simply by $Z^1_\lambda(A,G)$ the set of crossed homomorphisms with respect to $\mathrm{Inn}\,\tilde{\lambda}$.

Since $G \rtimes A = G \rtimes \tilde{\lambda}(A)$, Theorem 2.1 states that both $Z^1(A,G)$ and $Z^1_\lambda(A,G)$ correspond to the same set — the set of complements of G in $G \rtimes A$. This is a group-theoretic meaning of the following theorem.

Theorem 3.1 (Change of actions). *Let $\lambda \in Z^1(A,G)$. Then right multiplication by λ induces a bijection $\lambda_r\colon Z^1_\lambda(A,G) \to Z^1(A,G)$, which is defined by*

$$\lambda_r(\eta)(a) = \eta(a)\lambda(a) \quad \textit{for all } \eta \in Z^1_\lambda(A,G) \textit{ and } a \in A.$$

We often write $\lambda_r(\eta) = \eta \cdot \lambda$.

Let us determine the image of the coboundaries by this bijection λ_r. Set

$$B^1_\lambda(A,G) = \{[g,-]_\lambda \mid g \in G\},$$

where $[g,-]_\lambda\colon A \to G$ denotes the coboundary induced from g with respect to the action $\mathrm{Inn}\,\tilde{\lambda}$, i.e.,

$$[g,a]_\lambda = g \cdot {}^{\tilde{\lambda}(a)}(g^{-1}) \in G \leq G \rtimes A \quad \text{for all } a \in A.$$

We indicate $\lambda_r([g,-]_\lambda) = [g,-]_\lambda \cdot \lambda \in Z^1(A,G)$ by ${}^g\lambda$, so that

$$({}^g\lambda)(a) = [g,a]_\lambda \cdot \lambda(a) = {}^g(\tilde{\lambda}(a)) \cdot a^{-1}.$$

On the other hand, G acts on $\mathrm{Hom}(A, G \rtimes A)$ by

$${}^g\theta = \mathrm{Inn}(g) \circ \theta \quad \text{for } g \in G \text{ and } \theta \in \mathrm{Hom}(A, G \rtimes A).$$

Lemma 3.2. *Let $\lambda \in Z^1(A,G)$. Then we have*

(1) $\lambda_r(B^1_\lambda(A,G)) = \{{}^g\lambda \mid g \in G\}$.
(2) $\widetilde{{}^g\lambda} = {}^g\tilde{\lambda}$ *for any $g \in G$. (In other words, ${}^g\lambda$ is the 'G-part' of ${}^g\tilde{\lambda}$.)*

As the easiest case, we consider the zero map.

Lemma 3.3. *Let $0 \in Z^1(A,G)$ be the zero map. Then we have*

(1) $\tilde{0}\colon A \to G \rtimes A$ *is the inclusion map (the canonical monomorphism).*
(2) ${}^g0 = [g,-]$ *and* ${}^g\tilde{0} = \mathrm{Inn}(g)$ *on A for any $g \in G$.*

This implies the following at once:

Corollary 3.4. *All the complements of G in $G \rtimes A$ are conjugate if and only if $B^1(A,G) = Z^1(A,G)$.*

Note that any two conjugate complements of G in $G \rtimes A$ are conjugate by an element of G. We can also show the following by easy calculation:

Lemma 3.5. *For any $g, h \in G$, we have*

$${}^g[h,-] = [g,-]_{[h,-]} \cdot [h,-] = [gh,-].$$

3.2 Contravariant parameter A

Suppose that there is a short exact sequence of groups $1 \to B \to A \to \bar{A} \to 1$. We consider a problem whether there exists an *exact* sequence such as

$$1 \to Z^1(\bar{A}, G_?) \xrightarrow{\text{incl}} Z^1(A, G) \xrightarrow{\mathrm{res}_{A,B}} Z^1(B, G),$$

where $G_?$ is some subgroup of G on which B acts trivially, incl is the inclusion map, and $\mathrm{res}_{A,B}$ is the restriction map (although exactness of a sequence is not defined in the category of sets). Whereas we can not find such a common subgroup $G_?$, we can locally do as follows:

Theorem 3.6. *Suppose that $\mu \in Z^1(B, G)$ lies in $\mathrm{res}_{A,B}(Z^1(A, G))$, namely, $\mu = \mathrm{res}_{A,B}(\lambda)$ for some $\lambda \in Z^1(A, G)$. Then $\lambda_r \colon Z^1_\lambda(A, G) \to Z^1(A, G)$ induces a bijection*

$$\lambda_r \colon Z^1_\lambda(\bar{A}, C_G(\tilde{\mu}(B))) \to Z^1(A, G; B, \mu),$$

where we regard $Z^1_\lambda(\bar{A}, C_G(\tilde{\mu}(B))) \subseteq Z^1_\lambda(A, G)$ in a natural way, and where we set

$$Z^1(A, G; B, \mu) = \mathrm{res}^{-1}_{A,B}(\mu) = \left\{\tau \in Z^1(A, G) \mid \mathrm{res}_{A,B}(\tau) = \mu\right\}.$$

By Lemma 3.2, we have

Corollary 3.7. *Under the notation in Theorem 3.6, we have*

$$\lambda_r(B^1_\lambda(\bar{A}, C_G(\tilde{\mu}(B)))) = \left\{{}^h\lambda \mid h \in C_G(\tilde{\mu}(B))\right\}.$$

3.3 Covariant parameter G — Brauer's argument

Suppose that there is a short exact sequence of groups $1 \to K \to G \to K\backslash G \to 1$. We consider a similar problem whether there exists an exact sequence such as

$$1 \to Z^1(A, K_?) \xrightarrow{\text{incl}} Z^1(A, G) \xrightarrow{\text{mod } K} \mathrm{Map}(A, K\backslash G),$$

where $K_?$ is some subgroup of G, and Map denotes the set of maps, which may be replaced by Z^1 if K is A-invariant. For this problem, Brauer [6] gave an answer in the case where A is cyclic with trivial action on G, i.e., $Z^1(A, G) = \mathrm{Hom}(A, G)$. Moreover, it is remarkable that he assumed K is neither normal nor A-invariant. We can generalize his answer as follows.

For $K \leq G$ and $\lambda \in Z^1(A, G)$, let K_λ be the maximal $\tilde{\lambda}(A)$-invariant subgroup of K, namely,

$$K_\lambda = \bigcap_{a \in A} {}^{\tilde{\lambda}(a)}K.$$

Theorem 3.8. *Let K be a subgroup of G, and $\lambda \in Z^1(A, G)$. Then $\lambda_r \colon Z^1_\lambda(A, G) \to Z^1(A, G)$ induces a bijection*

$$\lambda_r \colon Z^1_\lambda(A, K_\lambda) \to \left\{\eta \in Z^1(A, G) \mid K\eta(a) = K\lambda(a) \ \textit{for all}\ a \in A\right\}.$$

By Lemma 3.2, we have

Corollary 3.9. *Under the notation in Theorem 3.8, we have*

$$\lambda_r(B^1_\lambda(A, K_\lambda)) = \left\{{}^k\lambda \mid k \in K_\lambda\right\}.$$

4 Applications

For given $B \le A$ and $g \in G$, we indicate the coboundary $[g,-]\colon B \to G$ by $[g,-]_B$ to avoid ambiguities, so that $\mathrm{res}_{A,B}([g,-]_A) = [g,-]_B$. Note that it always holds that

$$\mathrm{res}_{A,B}(B^1(A,G)) = B^1(B,G). \tag{$*$}$$

If n is an integer and A is abelian, then $A^n = \{a^n \mid a \in A\}$ is a subgroup of A. The following is a generalization of Brauer's lemma (Lemma 1.5).

Theorem 4.1. *Let A be a finitely generated abelian group and let G be a finite group. Then*

$$\mathrm{res}_{A,A^{|G|}}(Z^1(A,G)) = B^1(A^{|G|},G).$$

Proof. We use induction on the rank of A.

(1) Suppose that A is cyclic. We reduce this case to Hall's theorem (Theorem 1.3) as follows. Taking an epimorphism $F \simeq \mathbb{Z} \to A$, we have a commutative diagram

$$\begin{array}{ccc} Z^1(A,G) & \xrightarrow{\text{res}} & Z^1(A^{|G|},G) \\ {\scriptstyle\text{inf}}\big\downarrow & & {\scriptstyle\text{inf}}\big\downarrow \\ Z^1(F,G) & \xrightarrow{\text{res}} & Z^1(F^{|G|},G). \end{array}$$

This allows us to assume that $A = F$. Since $F \simeq \mathbb{Z}$, we have $|F : F^{|G|}| = |G| = |Z^1(F,G)|$. On the other hand, we have $B^1(F^{|G|},G) = \{[g,-]_{F^{|G|}} \mid g \in [G/C_G(F^{|G|})]\}$, where $[G/H]$ denotes a set of representatives for left cosets in G modulo a subgroup H. Thus, by definition,

$$\mathrm{res}^{-1}_{F,F^{|G|}}(B^1(F^{|G|},G)) = \biguplus_{g \in [G/C_G(F^{|G|})]} Z^1(F,G;F^{|G|},[g,-]_{F^{|G|}}).$$

However, Theorem 3.6 and usual argument for conjugation yield that

$$Z^1(F,G;F^{|G|},[g,-]_{F^{|G|}}) \simeq Z^1_{[g,-]}(F/F^{|G|},C_G({}^g(F^{|G|}))) \simeq Z^1(F/F^{|G|},C_G(F^{|G|})).$$

Therefore Hall's theorem implies that

$$\left|\mathrm{res}^{-1}_{F,F^{|G|}}(B^1(F^{|G|},G))\right| = \left|G : C_G(F^{|G|})\right| \cdot \left|Z^1(F/F^{|G|},C_G(F^{|G|}))\right| \equiv 0 \pmod{|G|},$$

which forces $\left|\mathrm{res}^{-1}_{F,F^{|G|}}(B^1(F^{|G|},G))\right| = |G| = |Z^1(F,G)|$, as desired.

(2) Suppose that $A = B \times C$ for nontrivial subgroups B and C, and $\lambda \in Z^1(A,G)$. By the equation $(*)$ and the inductive assumption, we have

$$\begin{aligned} B^1(B^{|G|},G) &= \mathrm{res}_{A,B^{|G|}}(B^1(A,G)) \\ &\subseteq \mathrm{res}_{A,B^{|G|}}(Z^1(A,G)) \subseteq \mathrm{res}_{B,B^{|G|}}(Z^1(B,G)) = B^1(B^{|G|},G), \end{aligned} \tag{$**$}$$

so that $\mathrm{res}_{A,B^{|G|}}(Z^1(A,G)) = B^1(B^{|G|},G)$. Hence $\lambda \in Z^1(A,G;B^{|G|},[h,-]_{B^{|G|}})$ for some $h \in G$. However, we have also $[h,-]_A \in Z^1(A,G;B^{|G|},[h,-]_{B^{|G|}})$. Theorem 3.6 yields that

$$[h,-]_r\colon Z^1_{[h,-]}(A/B^{|G|},C_G({}^h(B^{|G|}))) \to Z^1(A,G;B^{|G|},[h,-]_{B^{|G|}})$$

is bijective. Thus $\lambda = \eta \cdot [h,-]_A$ for some $\eta \in Z^1_{[h,-]}(A/B^{|G|}, C_G({}^h(B^{|G|})))$. Again applying induction to $C^{|G|} \le A/B^{|G|} \simeq (B/B^{|G|}) \times C$ as in (**), we have

$$\operatorname{res}_{A/B^{|G|},C^{|G|}}(Z^1_{[h,-]}(A/B^{|G|}, C_G({}^h(B^{|G|})))) = B^1_{[h,-]}(C^{|G|}, C_G({}^h(B^{|G|}))).$$

Hence there exists $g \in C_G({}^h(B^{|G|}))$ such that $\operatorname{res}_{A/B^{|G|},C^{|G|}}(\eta) = [g,-]_{[h,-]}$, the commutator of g with respect to the action $\mathrm{Inn}[h,-]^{\sim}$. This means that

$$\lambda(bc) = \eta(c)\cdot[h,bc] = [g,c]_{[h,-]}\cdot[h,bc] = [g,bc]_{[h,-]}\cdot[h,bc] \quad \text{for all } b \in B^{|G|},\ c \in C^{|G|}.$$

Consequently, $\operatorname{res}_{A,A^{|G|}}(\lambda) = [g,-]_{[h,-]}\cdot[h,-] = [gh,-]$ on $A^{|G|}$ by Lemma 3.5, as desired. □

As observed in Corollary 3.4, the second statement of the Schur-Zassenhaus theorem (Theorem 1.6) is equivalent to the following theorem, which can be reduced to the case where either A or G is abelian by the Feit-Thompson theorem and by our arguments.

Theorem 4.2. *If A and G are finite groups with* $\gcd(|A|,|G|) = 1$, *then* $Z^1(A,G) = B^1(A,G)$.

Proof. We use induction on $|A|$ and $|G|$. By the Feit-Thompson theorem, we may assume that either $A' \lneq A$ or $G' \lneq G$.

(1) Suppose that $A' \lneq A$, and consider the short exact sequence $1 \to A' \to A \to A/A' \to 1$. By induction, we have $Z^1(A',G) = B^1(A',G)$, so that

$$Z^1(A,G) = \biguplus_{h\in[G/C_G(A')]} Z^1(A,G;A',[h,-]_{A'}).$$

By applying Theorem 3.6 to $[h,-]_A \in Z^1(A,G;A',[h,-]_{A'})$,

$$[h,-]_r\colon Z^1_{[h,-]}(A/A', C_G({}^hA')) \to Z^1(A,G;A',[h,-]_{A'})$$

is bijective. However, A/A' is abelian and $(A/A')^{|H|} = A/A'$ for all $H \le G$ by hypothesis. Hence Theorem 4.1 implies that

$$Z^1_{[h,-]}(A/A', C_G({}^hA')) = B^1_{[h,-]}(A/A', C_G({}^hA')).$$

Consequently, it follows from Lemma 3.5 that every element of $Z^1(A,G)$ is of the form $[g,-]_{[h,-]}\cdot [h,-] = [gh,-]$ for some $g,h \in G$.

(2) Suppose that $G' \lneq G$, and consider the short exact sequence $1 \to G' \to G \to G/G' \to 1$. We have a natural map $Z^1(A,G) \to Z^1(A,G/G')$. However, G/G' is an A-module of order relatively prime to $|A|$. Hence it is well known in cohomology theory that $Z^1(A,G/G') = B^1(A,G/G')$. Therefore, for each $\lambda \in Z^1(A,G)$, there exists some $h \in G$ such that $G'\lambda(a) = G'[h,a]$ for all $a \in A$. By Theorem 3.8,

$$[h,-]_r\colon Z^1_{[h,-]}(A,G') \to \{\eta \in Z^1(A,G) \mid G'\eta(a) = G'[h,a] \text{ for all } a \in A\}$$

is a bijection. However, $Z^1_{[h,-]}(A,G') = B^1_{[h,-]}(A,G')$ by induction. Consequently, it follows from Lemma 3.5 that $\lambda = [g,-]_{[h,-]}\cdot[h,-] = [gh,-]$ for some $g \in G'$. □

As stated in the proof, this theorem is a generalization of a well known theorem in cohomology theory for A-modules G. Although we have used the Feit-Thompson theorem, the arguments of (1) and (2) in the proof are very parallel.

References

[1] T. Asai, N. Chigira, T. Niwasaki, and Y. Takegahara, *On the number of crossed homomorphisms* II, in preparation.

[2] T. Asai, T. Niwasaki, and Y. Takegahara, *Crossed homomorphisms from rank 2 abelian to exceptional p-groups*, J. Algebra **270** (2003), 212–237.

[3] T. Asai and Y. Takegahara, *On the number of crossed homomorphisms*, Hokkaido Math. J. **28** (1999), 535–543.

[4] ———, $|\mathrm{Hom}(A, G)|$, IV, J. Algebra **246** (2001), 543–563.

[5] T. Asai and T. Yoshida, $|\mathrm{Hom}(A, G)|$, II, J. Algebra **160** (1993), 273–285.

[6] R. Brauer, *On a theorem of Frobenius*, Amer. Math. Monthly **76** (1969), 562–565.

[7] W. Burnside, *The Theory of Groups of Finite Order*, 2nd ed., Cambridge University Press, 1907.

[8] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, 2nd ed., Pure and Appl. Math., Interscience Publishers, New York, 1966.

[9] M. Hall, *The Theory of Groups*, MacMillan, New York, 1959.

[10] P. Hall, *On a theorem of Frobenius*, Proc. London Math. Soc. (2) **40** (1935), 468–501.

[11] I. M. Isaacs and G. R. Robinson, *On a Theorem of Frobenius: Solutions of* $x^n = 1$ *in finite groups*, Amer. Math. Monthly **99** (1992), no. 4, 352–354.

[12] T. Yoshida, $|\mathrm{Hom}(A, G)|$, J. Algebra **156** (1993), 125–156.

[13] H. Zassenhaus, *The Theory of Groups*, 2nd ed., Chelsea Publishing Company, New York, 1958.